DEPARTMENT OF STATE

PRIVACY IMPACT ASSESSMENT
for
Immigrant Visa Allocation Management System (IVAMS)
May 2008

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Programs and Services
Privacy

E-mail: pia@state.gov

A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

1) Does this system collect, maintain or disseminate personally identifiable information about individual members of the public?**

YES X NO___

If answer is yes, please complete the survey in its entirety.

If answer is no, please complete the certification page and submit the completed PIA to: pia@state.gov.

2) Does a Privacy Act system of records already exist?

YES X NO

If yes, please provide the following:
System Name: Visa Records; Numbers: State-65 and State-722

3) What is the purpose of the system/application?

The Immigrant Visa Allocation Management System (IVAMS) is an inventory system for immigrant visas (IV) and diversity visas (DV). IVAMS tracks the Bureau of Consular Affairs (CA) posts' requests for, and allocations of, immigration and diversity visas. IVAMS also tracks the information associated with E3 visa types. The E3 information in IVAMS includes: the individual applicant's first name, middle name, last name; date of birth; country; and information from Form I-94, *Visa Waiver Nonimmigrant Arrival/Departure Document,* and address of petitioning company. The petitioning company is the source of the information. The U.S. Citizenship and Immigration Services (CIS) user enters the information into IVAMS-Web, which through data replication, is shared with IVAMS.

4) What legal authority authorizes the purchase or development of this system/application?

8 U.S.C 1101-1503 (Immigration and Nationality Act of 1952)

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

IVAMS covers individuals with E3 visa types. IVAMS also retains data from the DVIS system on individuals seeking a Diversity Visa. The system does not collect information on individuals applying for immigrant visas. However, through a database script, data from the DVIS system is moved into the IVAMS database for individuals applying for diversity visas.

2) What are the sources of the information in the system?

a. Who/what is the source of the information?
The individual seeking an E-3 non-immigrant status is the source of the information and is the person responsible for filling out the form. The U.S. Citizenship and Immigration Services (CIS) user enters the information into IVAMS-Web, which through data replication, is shared with IVAMS.

b. What type of information is collected from the source of the information?
The E3 information in IVAMS includes: the individual applicant's first, middle, and last name; date of birth; country; admission number from the Form I-94; and address of petitioning company.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?
The user enters this data through IVAMS Web. Verification checks are designed within the application. Verification checks and business logic designed into IVAMS Web is outlined in the IVAMS Web System Requirements Specification. If an invalid entry is made on the selection criteria page of an allocation request, a message will displays. The CIS user must correct the invalid entry and resubmit.

b. How will data be checked for completeness?
Refer to process as described in C3a above.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).
Data entered into IVAMS Web by Internet based users is reviewed by IVAMS internal users on OpenNet and is approved and accepted or rejected.

D. <u>INTENDED USE OF THE DATA:</u>

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?
Yes. Data collected is relevant and necessary for the purpose of managing visa allocation numbers.

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?
No new data is created.

Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?
No new data is created.

3) **Will the new data be placed in the individual's record?**
No new data is created.

4) **How will the new data be verified for relevance and accuracy?**
No new data is created.

5) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Personal data cannot be retrieved through the application interface; it can only be retrieved by a data base administrator (DBA) who has access to the personally identifiable information. DBAs retrieve data only upon request from the IVAMS data owner.

6) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
No reports are produced on individuals.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**
The system is operated in one site only.

2) **What are the retention periods of data in this system?**
IVAMS data is retained indefinitely within the system.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

The system does not collect information on individuals applying for immigrant visas. However, through a database script, data from the DVIS system is moved into the IVAMS database for individuals applying for diversity visas.

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
No.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**

N/A

6) If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?

Auditing data, such as an employee name, is collected for the purposes of auditing the visa application and adjudication process. Access to audit reports is limited to management personnel with a "need to know' based on user role .

IVAMS applications maintain audit records maintained within the IVAMS. The following table lists specific audited events and the information-captured content.

Mandatory	
Event	**Records**
User Action History	Records what the user did
User Activity History	Records userid, time of access, length of access and log off.

IVAMS audit information is stored in the Oracle database and can trace user actions to specific data elements. The audit information is sufficient to establish the events that occurred and who caused them. The audit information is only viewable by a user who has access to the tables that contain this information (i.e. the IVAMS ADMIN) and who has a working knowledge of SQL and can manually extract audit information from these tables.

The users are provided with printed audit logs every time an update or insert is performed against the database. Database audit logs are reviewed only when there are data integrity problems. The paper logs are kept from one to two weeks. The database logs are kept for as long as the data is kept in the database. Audit logs are protected from unauthorized modification, destruction, and access by the limited rights assigned by the system administrator using the operating system software. Only the information or system security officer (ISSO) and system/network managers are authorized to generate and view security-related audit logs.

7) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

The changes made to IVAMS do not require an amendment or revision to the existing Privacy Act system of records.

8) Are there forms associated with the system? YES NO _X__

F. ACCESS TO DATA:

1) Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

Access to data in IVAMS is restricted to domestic Bureau of Consular Affairs (CA) users and administrative users (database and system). Access to the personal identifiable information in IVAMS is limited to DBAs and the IVAMS business owner.

2) What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access is determined based on the user's role. User roles are assigned by CA management based on the job the employee will be performing. Only system administrators are allowed to create user roles.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

No. Users will not have access to all data within IVAMS. Access authorizations are based on the concept of separation of duties and least privilege. The IVAMS enforces separation of duties through assigned access authorizations in accordance with 12 FAM 629.2-1 and 12 FAM 643.2-1. Application security is controlled by enabling database accounts for each user and assigning roles for individual users. Based on the role defined for the user, the user is granted certain privileges in the database and the application. Access to the data and functions are controlled by the privileges granted to the roles. The roles are verified and set as the user logs into the application.

Each user will be assigned to a group based upon his/her functional requirements (i.e., Superusers, Operators, Data Entry, etc). Each group will be assigned access rights and privileges.

Only the IVAMS data base administrators have access to IVAMS.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)

IVAMS employs numerous controls to prevent the misuse of data by those having access including:

- Application roles that limit access to only those functions necessary for each user to complete job functions;
- Password protecting sensitive functions within the IVAMS application;
- Access to data base queries that can retrieve PII in IVAMS is not accessible to authorized users, except for the Chief of the IV Control & Rpt. Division;
- Auditing of all user activities; and
- Mandatory initial and annual refresher training on the proper handling of SBU data for all IVAMS users.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? **If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

Contract personnel are involved in the design and development of the IVAMS system. Privacy Act information is included in their contracts. All CA Bureau IVAMS contractors who handle SBU data are required to complete the standard cyber-computer security training given by the Bureau of Diplomatic Security and must acknowledge and comply with the established Rules of Behavior.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The IVAMS application interfaces with the following systems:

Name of System	Type of Data	Data Flow	Authorization Status
IVAMS-Web	Replication – Statistical Data Cutoff Dates	Bi-directional	ATO – Expiration Date 06/30/2007
Diversity Visa Information System (DVIS)	Batch - Statistical Data Allocation Approved	One direction from DVIS	ATO – Expiration Date 11/30/2008
Immigrant Visa Information System (IVIS)	Batch - Statistical Data Allocation Approved	One direction from IVIS	ATO – Expiration Date 05/31/2007
CCD	Replication – IVAMS data	One direction from IVAMS	ATO – Expiration Date 02/28/10

System and business owners are responsible for protecting the privacy rights of the public and employees affected by the interface.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**

There are no other agencies external to the Department of State who share or have access to data in IVAMS.

8) **Who is responsible for assuring proper use of the SHARED data?**

N/A